Responsible Office: Office of the Chief Information Officer

SUBJECT: Appropriate Use of NASA Langley Research Center (LaRC) Information Technology Resources

1. REFERENCES

a. NPD 2810.1, "Security of Information Technology."

b. NPR 2810.1, "Security of Information Technology."

2. SUMMARY

a. This directive sets forth NASA Langley Research Center (LaRC) policy and responsibilities for appropriate use of LaRC Information Technology (IT) Resources. Noncompliance with this LAPD may result in loss of access to LaRC IT resources.

b. Ultimately all NASA and contractor employees are individually responsible and accountable for proper and legal use of LaRC owned IT resources. We are also collectively responsible for protecting the public's confidence and financial investment in NASA.

3. POLICY

It is the policy of LaRC to:

a. Comply with prescribing NASA and Federal regulations on prohibited use.

b. Ensure that IT resources are used only for official Government business, emergency or authorized personal use.

(1) LaRC IT resources are provided for official business. Official business broadly includes any computer processing and communications that are required as part of the job. Official business includes, but is not limited to, the performance of NASA work-related duties in position descriptions, professional training and class work, work covered under grant agreements with NASA, tasks directed via NASA contracts, agreements with international partners, and support activities related to NASA contract tasking.

(2) LaRC management considers certain other activities to be within the scope of official business. For example, e-mail being used to distribute information about the following:

(a) Work-related events, such as technical symposiums, classes, and presentations.

This Document is Uncontrolled When Printed.
Check the LDMS Library via the LMS web site to verify that this is the correct version before use.

(b) Activities sponsored by the Center, such as the childcare center and carpooling.

(c) Events and activities specific to a particular Center sanctioned club or organization.

(d) Center-sanctioned activities, such as blood drives, sanctioned clubs, and organizations.

(3) Other use of IT resources, such as personal use of e-mail or the World Wide Web (WWW) for Internet access, is a privilege that may be rescinded if abused.

(4) Personal use of electronic mail is authorized under conditions similar to those for personal use of telephones. However, extensive personal use of e-mail on LaRC computers is not appropriate. When communications cannot reasonably be made during non-business hours or in emergency situations, employees may exchange brief e-mail messages with the following:

(a) Spouse or dependent.

(b) Someone responsible for the care of a spouse or dependent.

(c) Local government agencies.

(d) Physicians, dentists, and other medical practitioners.

(e) Businesses, such as those associated with home or auto repair.

(5) Limited personal use of the World Wide Web (WWW) is authorized as long as it does not interfere with the employee's work or the work of others. However, extensive personal use of the WWW on LaRC computers is not appropriate. Also, because of the drain on network resources, the reception of commercial radio or television broadcasts over the network is not permitted.

c. Use IT resources in a responsible manner so as not to place other LaRC IT resources at risk. Users of LaRC IT resources shall:

(1) Be authorized and sponsored by an LaRC organization.

(2) Maintain a valid e-mail account.

(3) Select a unique, non-trivial password, subject to the restrictions of the host computer. The password shall have at least eight characters and contain characters from at least three of the four character sets (upper case letters, lower case letters, numerals, and special characters). Passwords shall be protected from any form of disclosure and shall not be stored in files, function keys, or terminal logins. Passwords shall not be shared with anyone and shall be changed on a regular basis,

This Document is Uncontrolled When Printed.
Check the LDMS Library via the LMS web site to verify that this is the correct version before use.

commensurate with NASA policy on the protection of the category of information stored or processed on the host computer.

(4) Report any computer security weaknesses, incidents of possible misuse, or suspected security violations to line managers, system administrators, or the Center IT Security Manager (CITSM).

(5) Not download, install, or run security programs or utilities that may reveal any weaknesses in system security, such as sniffers, scanners or password cracking programs without the permission of the CITSM.

(6) Not divulge access information such as modem phone numbers or lists of accounts and users.

(7) Under no circumstances perform any moves, additions, alteration, or replacement of any LaRCNET connections, LaRC cable plant, or any other associated equipment.

(8) Not purposely engage in activities to:

(a) Harass other users.

(b) Degrade system performance.

(c) Deprive an authorized user access to a resource.

(d) Obtain resources beyond those allocated to you.

(e) Circumvent computer security measures.

(f) Attempt to gain access to data or systems for which proper authorization has not been granted.

4. APPLICABILITY

This LAPD applies to all LaRC employees, all LaRC contractor and subcontractor employees, and all other individuals authorized access to LaRC IT resources with authentication requirements.

5. RESPONSIBILITIES

Specific responsibilities of individuals and organizations with regard to the appropriate use of LaRC IT resources are as follows:

a. LaRC Chief Information Officer

This Document is Uncontrolled When Printed.
Check the LDMS Library via the LMS web site to verify that this is the correct version before use.

(1) Ensure that LaRC IT policies contribute to the secure operation and protection of LaRC systems and information.

(2) Issue Center IT security policies and guidelines.

b. LaRC Center Information Technology Security Manager

(1) Develop Center IT security policies and guidelines for approval and issuance by the LaRC CIO.

(2) Develop and implement the Center IT security guidelines.

(3) Investigate incidents of suspected inappropriate use in cooperation with the Office of Human Resources, Office of Security and Public Safety, Office of Chief Counsel, Office of Inspector General, and appropriate supervisory personnel.

c. Network and Computer Services Branch (NSCB), OCIO

Manage, operate, and deploy LaRC's computer network.

d. Supervisors

(1) Implement LaRC's policies in managing IT resources.

(2) Review employee use of IT resources and applying appropriate internal controls to ensure that only those individuals who require access to LaRC IT resources have such access.

e. Employees

Use LaRC IT resources only for official business, emergency, and other approved activities.

f. Contracting Officer's Technical Representative

Responsible for the proper management of IT resource use by contractor personnel.

6. RECISION

LAPD 2810.1, dated January 13, 2000.

Jeremiah F. Creedon
Director

This Document is Uncontrolled When Printed.
Check the LDMS Library via the LMS web site to verify that this is the correct version before use.